PHISHING

Maria Esther Condori Velasquez
Universidad Mayor de San Andrés
Carrera de Informática
Analisis y Diseño de Sistemas de Información
marithe.c.14@gmail.com

RESUMEN

El "phishing" consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude**.**

Una de las modalidades más peligrosas del phishing es el pharming. Esta técnica consiste en modificar el sistema de resolución de nombres de dominio (DNS) para conducir al usuario a una página web falsa, de esta manera hacen "creer" a la posible víctima que realmente los datos solicitados proceden del sitio "Oficial" cuando en realidad no lo es.

Palabras Clave

Phishing, pagina web, estafadores, información personal, prevención.

1. INTRODUCCIÓN

Phishing es denominado un tipo de delito dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta, con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantáneao incluso utilizando también llamadas telefónicas.

Un nuevo ataque de phishing se basa en colocar una etiqueta HTML en un servicio vulnerable para capturar los datos de autenticación de los usuarios.

2. TECNICAS DE PHISHING

La mayoría de los métodos de phishing utilizan:
- Manipulación en el diseño del correo electrónico para lograr que un enlace parezca una ruta legítima de la organización por la cual se hace pasar el impostor.

- URLs manipuladas, o el uso de subdominios, son trucos comúnmente usados por phishers.

- Utilizar direcciones que contengan el carácter arroba: @, para posteriormente preguntar el nombre de usuario y contraseña, este método ha sido erradicado desde entonces en los navegadores de Mozillae Internet Explorer.

- Utilizan comandos en JavaScripts para alterar la barra de direcciones. Esto se hace poniendo una imagen de la URL de la entidad legítima sobre la barra de direcciones, o cerrando la barra de direcciones original y abriendo una nueva que contiene la URL ilegítima.

- Los atacantes simplemente necesitan controlar un servidor donde almacenan la imagen y algo de código adicional.Entonces inyectan la etiqueta HTML, supuestamente inofensiva dentro del servicio vulnerable.

Nombre de dominio internacionalizado (IDN) en los navegadores, puesto que puede ser que direcciones que resulten idénticas a la vista puedan conducir a diferentes sitios. Al usar esta técnica es posible dirigir a los usuarios a páginas web con malas intenciones.

- SMS (mensaje corto); La recepción de un mensaje donde le solicitan sus datos personales.

- Llamada telefónica; Pueden recibir una llamada telefónica en la que el emisor suplanta a una entidad privada o pública para que usted le facilite datos privados.
- Página web o ventana emergente; es muy clásica y bastante usada. En ella se simula suplantando visualmente la imagen de una entidad oficial, empresas, etc. pareciendo ser las oficiales.

3. FASES

- En la primera fase, la red de estafadores se nutre de usuarios de chat, foros o correos electrónicos, a través de mensajes de ofertas de empleo con una gran rentabilidad o disposición de dinero (hoax o scam). En el caso de que caigan en la trampa, los presuntos intermediarios de la estafa, deben rellenar determinados campos, tales como: Datos personales y número de cuenta bancaria.
- En la segunda fase se comete el phishing, ya sea el envió global de millones de correos electrónicos bajo la apariencia de entidades bancarias, solicitando las claves de la cuenta bancaria (*phishing*) o con ataques específicos.
- El tercer paso consiste en que los estafadores comienzan a retirar sumas importantes de dinero, las cuales son transmitidas a las cuentas de los intermediarios. Los intermediarios realizan el traspaso

a las cuentas de los estafadores, llevándose éstos las cantidades de dinero.

4. DAÑOS CAUSADOS POR EL PHISHING

Los daños causados por el phishing oscilan entre la pérdida del acceso al correo electrónico a pérdidas económicas sustanciales. Este tipo de robo de identidad se está haciendo cada vez más popular por la facilidad con que personas confiadas normalmente revelan información personal a los phishers, incluyendo números de tarjetas de crédito y números de seguridad social. Una vez esta información es adquirida, los phishers pueden usar datos personales para crear cuentas falsas utilizando el nombre de la víctima, gastar el crédito de la víctima, o incluso impedir a las víctimas acceder a sus propias cuentas.

5. MEDIDAS DE PREVENCIÓN PARA EVITAR SER VÍCTIMA DEL PHISHING

- ✓ Si recibe un correo electrónico que le pide información personal o financiera, no responda.
- ✓ Si el mensaje lo invita a acceder a un sitio web a través de un enlace incluido en su contenido, no lo haga.
- ✓ No envié información personal usando mensajes de correo electrónico.
- ✓ No acceda desde lugares públicos
- ✓ Verifique los indicadores de seguridad del sitio web en el cual ingresa información personal.
- ✓ Mantenga actualizado el software de su PC.
- ✓ Revise sus resúmenes bancarios y de tarjetas de crédito tan pronto los reciba.
- ✓ No descargue ni abra archivos de fuentes no confiables.
- ✓ No conteste ningún mensaje que resulte sospechoso.
- ✓ Permanezca siempre atento para evitar el acceso indebido a su información personal.

6. CONCLUSIÓN

La mejor manera de protegerse del phishing es tomar en cuenta de que manera actúan los proveedores de servicios financieros y otras entidades susceptibles de recibir este tipo de ataques.
Mantenerse informados con las nuevas tendencias y tipos de ataques de phishing para prevenir las estafas que realizan, tomando en cuenta la medida de prevención.

7. REFERENCIAS

[20] Joachim B. Ataques de autenticación multiplataforma. 2005[Disponible en:]. http://seguridad.internautas.org/html/451.html. [Fecha de búsqueda:] 09/04/13

[21] Medidas de prevención para evitar ser víctima del “phishing”. [Disponible en:]. http://www.seguridad.unam.mx/documento/?id=7#Benefits. [Fecha de búsqueda:] 09/04/13

[22] Phishing. [Disponible en:]. http://www.alertaenlinea.gov/articulos/s0003-phishing. [Fecha de búsqueda:] 09/04/13

[23] Qué es el phishing. 2005.[Disponible en:]http://www.infospyware.com/articulos/que-es-el-phishing/. [Fecha de búsqueda:] 15/04/13

Qué es el phishing y cómo protegerse. [Disponible en:]http://seguridad.internautas.org/html/451.html. [Fecha de búsqueda:] **15**/04/13